

Gordon M. Fauth, Jr. (SBN 190280)
gfauth@finkelsteinthompson.com
Of Counsel
Rosanne L. Mah (Cal. Bar No. 242628)
rmah@finkelsteinthompson.com
Of Counsel

FINKELSTEIN THOMPSON LLP

100 Pine Street, Suite 1250
San Francisco, California 94111
Direct Telephone: (510) 238-9610
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

Attorneys for Individual and Representative
Plaintiff Malcolm B. Feied

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
San Francisco-Oakland Division

MALCOLM B. FEIED, an Individual, on behalf of
himself and all others similarly situated,

Plaintiff,

vs.

EQUIFAX, INC., a Corporation,

Defendant.

Case No.

**CLASS ACTION COMPLAINT
FOR DAMAGES AND
EQUITABLE RELIEF**

JURY TRIAL DEMANDED

Plaintiff Malcolm B. Feied, individually and on behalf of all others similarly situated, by and through his undersigned counsel, for his complaint brings this class action for damages and equitable relief against Defendant Equifax, Inc. Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge:

NATURE OF THE ACTION

1
2 1. This is a civil action brought by Plaintiff Malcolm B. Feied (“Feied” or
3 “Plaintiff”) on behalf of himself and all others similarly situated against Defendant Equifax, Inc.
4 (“Equifax” or “Defendant”).

5 2. Equifax is one of the largest consumer credit reporting agencies in the United
6 States and the world. As such, Equifax receives, collects and maintains sensitive personal
7 information belonging to and concerning hundreds of millions of consumers, which it keeps in
8 its computer databases.

9 3. On or about September 7, 2017, Equifax announced that it had experienced a
10 massive data breach affecting some 143 million consumers in the United States, some 15 million
11 of them California citizens (hereafter, “data breach”). Equifax stated the breach happened
12 because of a vulnerability in one of its website applications. Because of the data breach, which
13 Equifax says occurred from May through July 2017, Plaintiff’s and consumers’ personal
14 information, including names, addresses, telephone numbers, social security numbers, drivers’
15 license numbers, credit card numbers and other information is now in the hands of unknown
16 hackers and may be used for identity theft and other injurious purposes.

17 4. Plaintiff and consumers in California and across the United States have suffered
18 harm because of Defendant’s failure to take adequate security measures to protect their data and
19 failure to prevent hackers from gaining access to such sensitive information, Defendant’s failure
20 to disclose to Plaintiff and others that it did not adequately protect information entrusted to it or
21 over which it has control, and failure to disclose the occurrence of the breach until months after it
22 occurred. The situation is made the more egregious by the fact that Equifax has suffered serious
23 data breaches in the past and was on notice of the need to take effective measures to prevent such
24 a breach. Equifax willfully chose not to take the measures that it knew were necessary to protect
25 the sensitive data in its keeping, and the direct result is the largest consumer data breach of its
26 kind in history, given the scale and the scope of the personal information taken.

27 5. Defendant’s actions and omissions violate laws including the Fair Credit
28 Reporting Act, 15 U.S.C. § 1681 *et seq.*, the Security Breach Notification Law, Cal. Civil Code §
1798.82; the Customer Records Act, Cal. Civ. Code § 1798.81.5; the Unfair Competition Law,

1 Cal. Bus. and Prof. Code §§ 17200, *et seq.*; and constitute negligence.

2 6. Accordingly, Plaintiff brings this case as a class action and, on behalf of himself
3 and other similarly situated persons, seeks damages including compensatory damages, statutory
4 and punitive damages, injunctive and equitable relief, declaratory relief, and attorney fees and
5 costs.

6 **JURISDICTION AND VENUE**

7 7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because a
8 claim under federal law is pleaded, and pursuant to the Class Action Fairness Act, 28 U.S.C. §
9 1332(d), because the aggregate amount in controversy exceeds \$5 million, exclusive of interests
10 and costs; the number of members of each of the proposed Classes exceeds 100; and Plaintiff and
11 many members of the proposed Plaintiff Classes are citizens of different states than the
12 Defendant.

13 8. This Court has personal jurisdiction over the Defendant as it conducts substantial
14 business in the State of California and in this Judicial District and/or the conduct complained of
15 occurred in and/or emanated from this State and Judicial District.

16 9. Venue is proper in this Judicial District because Defendant conducts substantial
17 business in this Judicial District, Plaintiff is a resident of the Judicial District, and/or the conduct
18 complained of occurred in or emanated from this District.

19 **INTRADISTRICT ASSIGNMENT**

20 10. Venue is proper in this Judicial District and the Oakland/San Francisco division
21 thereof pursuant to 28 U.S.C. section 1391 subsections (b) and (c), and Civil L.R. 3-2
22 subsections (c) and (d). Plaintiff resides in Alameda County within such division, and Defendant
23 transacts business in this division and County and/or a substantial part of the events giving rise to
24 the claims at issue in the litigation arose in this division and County.

25 **PARTIES**

26 11. Plaintiff Malcolm B. Feied is and has at all relevant times been a resident of
27 Alameda County, California and of this Judicial District.

28 12. According to Equifax, Feied's personal data is implicated in the data breach. As a
result of the theft of his personal data in the data breach, he is now forced to expend time, effort

1 and resources in monitoring activities involving his personal finances and use of his identity and
2 personal information.

3 13. Defendant Equifax, Inc. is a Georgia corporation with headquarters in Atlanta,
4 Georgia. Its main business consists of, for monetary fees, assembling and/or evaluating
5 consumer credit information or other information on consumers for the purposes of furnishing
6 consumer reports to third parties.

7 14. Equifax was founded in 1899. Operating throughout the world, it compiles and
8 handles sensitive personal information belonging to millions of consumers worldwide. Equifax
9 operates throughout the United States, with extensive operations in California and this Judicial
10 District, including having multiple offices in this Judicial District. Equifax's wholly-owned
11 subsidiary, TrustedID, Inc., which Equifax involved in the aftermath of the data breach in an
12 attempt to control damage and garner more business from the breach, is located in Palo Alto,
13 California.

14 **SUBSTANTIVE ALLEGATIONS COMMON TO ALL CAUSES OF ACTION**

15 **Defendant Knew of the Massive Data Breach for At Least Six Weeks, and Possibly**
16 **Much Longer, But Failed to Notify Affected Consumers or the Public**

17 15. Equifax is the oldest of the three largest providers of consumer credit information
18 in the United States. As Equifax states in its published reports, the company organizes,
19 assimilates and analyzes data on more than 820 million consumers and more than 91 million
20 businesses worldwide. It solicits, receives and/or collects consumer data from a variety of
21 sources, including directly from consumers, from businesses and financial institutions, and from
22 more than 7,100 employers. It employs approximately 9,500 employees worldwide.

23 16. Equifax maintains sensitive personal and financial information on many millions
24 of consumers in the United States, including Plaintiff and members of the proposed Classes. It
25 maintains their information in electronic databases. It uses such information to provide credit
26 reports and other reports to third parties, for its own profit.

27 17. On September 7, 2017, Equifax issued a press release announcing that its
28 information security systems had been hacked in a massive data breach, lasting from May
through July 2017, exposing approximately 143 million U.S. consumers' sensitive and personal

1 information. The information taken by unknown hackers includes names, street addresses, birth
2 dates, social security numbers, driver's license numbers, financial information, credit card
3 information and other personal information ("Personal Information"). The data breach exposed
4 the Personal Information of some 15 million consumers in California alone.

5 18. In terms of size and the scope of the consumer data taken, the Equifax data breach
6 is unparalleled. While a few other data breaches have been larger in sheer size, the Equifax
7 breach is by far the worst to date in terms of harm to consumers, given the detailed personal
8 information it has provided to the cyberthieves. "On a scale of 1 to 10 in terms of risk to
9 consumers, this is a 10," said Avivah Litan, a fraud analyst at Gartner Research.

10 19. The September 7, 2017 press release was the first notice Plaintiff and other
11 consumers received that their Personal Information was in jeopardy.

12 20. According to Equifax, the data breach began as early as mid-May 2017. Equifax
13 has confirmed that at that time hackers entered its system through a web-application
14 vulnerability. Equifax says it became aware of the breach on July 29, 2017. However, according
15 to a September 18, 2017 Bloomberg report, Equifax became aware of a serious security breach in
16 March 2017, four months earlier than reported by Equifax. While acknowledging the March
17 2017 intrusion, Equifax has denied it was part of the later data breach.

18 21. Even according to its own timeline, Equifax took approximately six weeks to
19 notify the public about the massive data breach. When Equifax finally announced the
20 cybersecurity incident, it directed consumers to visit a Equifax breach notification website,
21 www.equifaxsecurity2017.com to find out if their personal information had been taken.

22 22. Incredibly, in addition to waiting to notify consumers of the danger to which it
23 had exposed them, Equifax then attempted (and is attempting) to use the data breach as a
24 business opportunity to enroll consumers in a service that will generate more profit for itself and
25 a wholly-owned subsidiary.

26 23. At the www.equifaxsecurity2017.com website to which Equifax directed
27 consumers, in addition to telling consumers who entered the requested information whether their
28 personal information was implicated in the data theft, Equifax also involved a company call
TrustedID in damage control, attempting to induce affected consumers to have TrustedID

1 monitor credit activities for them. In enticing affected consumers to enroll with TrustedID, it
2 failed to disclose that TrustedID, based in Palo Alto, California, is its wholly-owned subsidiary,
3 or that the terms of the user agreement for the credit monitoring service would require consumers
4 to arbitrate disputes with TrustedID and Equifax and would prevent them from bringing an
5 action in court (Equifax later stated that it would not seek to enforce the arbitration agreement
6 with respect to the data breach).

7 24. Despite having been aware of the massive data breach since at least July 2017 and
8 possibly as early as March 2017, Equifax has not yet individually notified consumers whose
9 Personal Information has been allowed to fall into the hands of hackers, to provide them the
10 details of the theft of their personal information as required by law.

11 25. While Equifax was at least weeks and possibly months late in notifying the public
12 of the data breach, and while it still has not proactively provided individual notification to
13 affected consumers, certain of its executives allegedly took steps to protect their own financial
14 interests before the breach was made public.

15 26. The Department of Justice has reportedly opened a criminal investigation into
16 whether three top Equifax officials violated insider trading laws when they sold company stock
17 before the massive cyber breach was disclosed publicly. According to Bloomberg News, Federal
18 prosecutors are examining nearly \$1.8 million in sales of Equifax stock by chief financial officer
19 John Gamble, Joseph Loughran, president of Equifax's information solutions division, and
20 Rodolfo Ploder, president of its workforce solutions unit.

21 **Defendants' Inadequate Security Measures and Willful and Negligent Practices**

22 27. The data breach was a direct result of Equifax's willful failure to employ
23 reasonable security measures to protect consumers' Personal Information from unauthorized
24 access, including implementation of security measures and technological safeguards to prevent
25 this type of attack and maintenance of security protocols to detect and halt the unauthorized
26 accesses.

27 28. As the oldest of the three largest credit reporting agencies, Equifax knew that it
28 was constantly at risk of cyber attacks aimed at stealing consumers' Personal Information. Yet,
in spite of knowing that the Personal Information it had collected from consumers was targeted

1 by cyber thieves, Equifax failed to implement proper security procedures and protocols that are
2 standard in the industry and which would have prevented the data breach.

3 29. Equifax was on notice that its existing security measures were inadequate
4 because it had already experienced multiple serious data breaches—all caused by inadequate
5 security procedures and measures—in which consumers’ personal information was accessed by
6 unauthorized third parties.

7 30. In September 2015, Equifax confirmed that hackers had broken into one of its
8 servers and stolen data belonging to 15 million consumers, including names, dates of birth,
9 addresses, Social Security numbers and/or drivers’ license numbers, and other sensitive
10 information.

11 31. In May 2016, Equifax's W-2 Express website suffered an attack that resulted in
12 the theft of 430,000 names, addresses, social security numbers and other personal information of
13 retail firm Kroger. This resulted in a class action which alleged that Equifax had “willfully
14 ignored known weaknesses in its data security, including prior hacks into its information
15 systems.”

16 32. In spite of these and other previous incidents in which hackers gained access to its
17 system, and in spite of industry warnings that its consumer databases were vulnerable, Equifax
18 willfully chose not to implement security measures to prevent this type of attack. Among other
19 things, Equifax allowed a website application vulnerability to exist--which it says caused the data
20 breach--while easily implemented patches and security measures would have prevented or
21 eliminated that vulnerability. Equifax also chose not to implement security protocols that would
22 have detected the unauthorized accesses and halted or limited the size and scope of the data
23 breach.

24 33. As a result of its willful, reckless and/or negligent acts and omissions, Equifax has
25 once again exposed personal information of consumers to online hackers--this time in a massive
26 consumer data breach of unprecedented proportions given the size of the breach and the scope of
27 the personal information taken.
28

**Plaintiff and the Class Have Suffered an Injury in Fact That Will
Endanger Them For Many Years to Come, if not Forever**

34. As a result of the data breach, Plaintiff's and consumers' Personal Information is now in the hands of unknown hackers, and Plaintiff and the Class now face an imminent heightened, and substantial risk of identity theft and other fraud, which is a concrete and particularized injury traceable to Defendant's conduct. Accordingly, Plaintiff and the Class have suffered "injury-in-fact." *See Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C.Cir. 2017).

35. Theft of personal information is a serious and growing problem in the United States. The 2017 Identity Fraud Report by Javelin Strategy & Research reports that, "2016 will be remembered as a banner year for fraudsters as numerous measures of identity fraud reached new heights." According to Javelin, the overall identity fraud incidence rose 16% to affect 6.15% of U.S. consumers—the highest on record—with 15.4 million U.S. identity theft victims, who lost a total of \$16 billion.

36. Identity theft is a growth industry. As tracked by the Consumer Sentinel Network, maintained by the Federal Trade Commission, of the 3.1 million consumer fraud complaints filed with law enforcement and private agencies in 2015, 16 percent related to identity theft, with identity theft complaints increasing by more than 47 per cent from 2014.

37. According to a Javelin study, there is a high correlation between having information taken in a data breach and becoming an identity theft victim, with nearly 1 in 4 data breach letter recipients becoming an actual victim of identity fraud. Breaches involving theft of Social Security numbers were found to be the most dangerous.

38. The personal information Equifax allowed hackers to take is particularly dangerous in the hands of ID thieves. That is because it includes sensitive personal information, such as names and addresses, Social Security numbers, birth dates, credit card numbers, driver's license numbers, and other identity information that can be used for identity theft and fraud but which cannot be easily changed or cancelled by Plaintiff and other consumers. In fact, the combination of information stolen in the data breach would be fully sufficient to misappropriate a person's identity for the purpose of opening new accounts, obtaining loans, incurring charges, or engaging in various other financial frauds.

39. Plaintiff and other affected consumers are at much greater risk as a result of the Equifax data breach than if only their credit card information or bank account information had been stolen. Bad as that kind of theft can be, credit cards and bank accounts can be frozen or cancelled quickly and new numbers issued, and that can be accomplished as easily as by making a telephone call to the financial institution. Here by contrast, the Personal Information stolen includes personal identity information that either cannot be changed at all, or only with great difficulty and delay. As a result, Plaintiff and Class members will be forced to live under the threat of ID theft and fraudulent use of their personal data for years to come, and face protracted battles in protecting their good names and financial integrity against the misuse of their Personal Information that is now in the hands of fraud artists and identify thieves.

40. As reported by USA Today, the data breach will endanger and haunt Plaintiff and Class members for many years to come and possibly forever:

Once hackers gain access to these key pieces of personal data -- which is akin to the DNA of a person's online digital self -- it is at the cyber thieves' disposal forever to cause harm.

"It's very problematic for hackers to have all that important information all in one place," says John Ulzheimer, a credit expert who once worked for Equifax and credit-score firm FICO. "This information is perpetually valuable. You are not going to change your name or date of birth or Social Security number. In five years they will be the same, unlike a credit card that takes five minutes to cancel over the phone."

...

The bad news is "this data will be used for years," says Avivah Litan, a security analyst at Gartner. "So, as a consumer, you need to be hyper-vigilant."

-- "Equifax Data Breach Could Create Lifelong Identity Theft Threat," USA Today (Sept. 9, 2017), *found at* <https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/>.

41. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves can use stolen personal information such as social security numbers to open financial accounts, receive government benefits and incur charges and credit in the victim's name. See <http://www.gao.gov/new.items/d07737.pdf>. As the GAO Report states, this type of identity theft is the most harmful because it may take

1 considerable time for the victim to become aware of the theft and can adversely impact the
2 victim's credit rating. In addition, the GAO Report states that victims of identity theft will face
3 "substantial costs and inconveniences repairing damage to their credit records...[and their] good
4 name."

5 42. According to the Federal Trade Commission ("FTC"), identity theft victims must
6 spend countless hours and money repairing the impact to their good name and credit record.
7 Identity thieves use stolen personal information such as social security numbers for a variety of
8 crimes, including credit card fraud, phone or utilities fraud, tax fraud, and bank/finance fraud.
9 See <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>.

10 43. It can be expensive for consumers to rectify identify theft. A recent report
11 sponsored by Experian states that the "average total cost to resolve an identity theft-related
12 incident ... came to about \$20,000." Forty percent of consumers said they were never able fully
13 to resolve their identity theft.

14 44. Identity theft crimes often involve more than financial loss, causing harm such as
15 loss of reputation, adverse credit reports, and even criminal records. Identity thieves can use the
16 victim's identity to obtain a driver's license or other licenses; commit fraud and other crimes
17 exposing the victim to arrest; and create adverse employment, house rental and other history for
18 the victim.

19 45. It is also a crime that has effects far beyond the date of the theft. A person whose
20 personal information has been compromised may not see any signs of identity theft for years.
21 According to the GAO Report: "stolen data may be held for up to one year or more before being
22 used to commit identity theft."

23 46. Identity theft criminals can easily sell or trade the stolen personal information on
24 the cyber black-market. There are web sites where the stolen information is marketed
25 surprisingly freely, according to industry sources. See
26 <http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/>. There are
27 also more clandestine web sites, unlisted by search engines and based in foreign countries, and
28 on the so-called "dark web," where blocks of stolen identity information are traded or sold to
anonymous buyers. Often the transactions are in bitcoin or utilize other untraceable methods of

1 payment.

2 47. Equifax was targeted for the data theft precisely because the Personal Information
3 it stores is so sensitive and comprehensive as to be valuable for the purpose of identity theft.
4 Thus, there is a heightened and substantial risk the information has already been, or will be, sold
5 and used for identity theft purposes.

6 48. The injury to Plaintiff and the Classes is fairly traceable to Equifax, because
7 Equifax failed properly to secure their data, subjecting them to the substantial risk of identity
8 theft.

9 49. For all of the above reasons, Plaintiff and the Classes have suffered harm; and
10 there is a substantial risk of injury to Plaintiff and the Class that is imminent and concrete and
11 that will continue for years to come.

12 CLASS ACTION ALLEGATIONS

13 50. Plaintiff brings this action on behalf of himself and on behalf of two classes--a
14 National Class and a California Class (together "Classes").¹

15 51. The National Class is initially defined as follows:

16 **"All persons in the United States whose Personal Information was exposed**
17 **due to the cyber attack disclosed by Equifax on or about September 7, 2017."**

18 Excluded from the National Class are Defendant, its corporate parents, subsidiaries,
19 officers, directors, employees, and partners.

20 52. The California Class is initially defined as follows:

21 **"All persons who reside in California whose Personal Information was**
22 **exposed due to the cyber attack disclosed by Equifax on or about September**
23 **7, 2017."**

24 Excluded from the California Class are Defendant, its corporate parents, subsidiaries,
25 officers, directors, employees, and partners.

26 53. This action has been properly brought and may properly be maintained as a class

27
28 ¹ If not otherwise clear from the context, "Class" not preceded by "National" or "California"
means and includes both the National and California Classes.

1 action under Rule 23(a)(1-4), Rule 23(b)(1), (2) or (3), and/or Rule 23(c)(4) of the Federal Rules
2 of Civil Procedure and case law thereunder.

3 **Numerosity of the Classes**

4 **(Fed. R. Civ. P. 23(a)(1))**

5 54. Members of each Class are so numerous that their individual joinder is
6 impractical. The Classes comprise, at the least, millions of consumers. Approximately 143
7 million consumers nationwide, including some 15 million consumers in California, had their
8 Personal Information exposed in the data breach. The precise number of the members of each
9 Class, and their addresses, are unknown to Plaintiff at this time, but can be ascertained from
10 Defendant's records. Members of the Classes may be notified of the pendency of this action by
11 mail or email, supplemented (if deemed necessary or appropriate by the Court) by published
12 notice.

13 **Predominance of Common Questions of Fact and Law**

14 **(Fed. R. Civ. P. 23(a)(2); 23(b)(3))**

15 55. Common questions of law and fact exist as to all members of the Classes. These
16 questions predominate over the questions affecting only individual members of the Classes. The
17 common legal and factual questions include, without limitation:

18 (a) Whether Defendant represented that consumers' personal information in
19 its custody was secure when in fact it was not;

20 (b) Whether Defendant failed to disclose that personal information entrusted
21 to it was at risk of theft owing to Defendant's inadequate security procedures;

22 (c) Whether, Defendant failed to maintain reasonable procedures designed to
23 limit the furnishing of consumer reports, including the Personal Information, to only those
24 purposes listed in 15 U.S.C. § 1681b;

25 (d) Whether Defendant failed to implement and maintain reasonable security
26 measures and procedures, appropriate to the information in its custody, to safeguard Class
27 members' personal information, in violation of California Civil Code section 1798.81.5(b);

28 (e) Whether Defendant was negligent in its handling and protection of Class
members' personal information;

(f) When Defendant became aware of the data breach;

(g) Whether Defendant notified Class members of the data breach without unreasonable delay as required by California Civil Code section 1798.82;

(h) Whether Defendant's practices, actions and omissions constitute unlawful, fraudulent and/or unfair business practices in violation of California Business and Professions Code section 17200 *et seq.*;

(i) Whether Defendant was negligent with respect to the safekeeping of the Personal Information in its databases; and

(j) The nature of the relief, including damages and equitable relief, to which Plaintiff and members of the Classes are entitled.

Typicality of Claims

(Fed. R. Civ. P. 23(a)(3))

56. Plaintiff's claims are typical of the claims of the Classes because Plaintiff, like all other Class members, had his personal information in Defendant's custody exposed in the security breach.

Adequacy of Representation

(Fed. R. Civ. P. 23(a)(4))

57. Plaintiff is an adequate representative of the Classes, because his interests do not conflict with the interests of the members of the Classes and he has retained counsel competent and experienced in complex class action and consumer litigation.

58. The interests of the members of the Classes will be fairly and adequately protected by Plaintiff and his counsel.

Superiority of a Class Action

(Fed. R. Civ. P. 23(b)(3))

59. A class action is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and members of the Classes. The damages suffered by each individual members of the Classes, while significant, are small given the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. Further, it would be virtually impossible for the members of the Classes

1 individually to redress effectively the wrongs done to them. And, even if members of the
2 Classes themselves could afford such individual litigation; the court system could not, given the
3 thousands or even millions of cases that would need to be filed. Individualized litigation would
4 also present a potential for inconsistent or contradictory judgments. Individualized litigation
5 would increase the delay and expense to all parties and the court system, given the complex legal
6 and factual issues involved. By contrast, the class action device presents far fewer management
7 difficulties and provides the benefits of single adjudication, economy of scale, and
8 comprehensive supervision by a single court.

9 **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness**
10 **of Final Injunctive or Declaratory Relief**

11 **(Fed. R. Civ. P. 23(b)(1) And (2))**

12 60. In the alternative, this action may properly be maintained as a class action with
13 respect to each Class, because:

14 (a) the prosecution of separate actions by individual members of the Classes
15 would create a risk of inconsistent or varying adjudication with respect to individual Class
16 members, which would establish incompatible standards of conduct for the Defendant; or

17 (b) the prosecution of separate actions by individual Class members would
18 create a risk of adjudications with respect to individual members of the Classes which would, as
19 a practical matter, be dispositive of the interests of other members of the Classes not parties to
20 the adjudications, or substantially impair or impede their ability to protect their interests; or

21 61. (c) Defendant has acted or refused to act on grounds generally applicable to
22 the Classes, thereby making appropriate final injunctive or corresponding declaratory relief with
23 respect to each Class as a whole.

24 **Issue Certification**

25 **(Fed. R. Civ. P. 23(c)(4))**

26 62. In the alternative, common questions of fact and law, including those set forth in
27 Paragraph 55 above, are appropriate for issue certification.
28

FIRST CAUSE OF ACTION

(Willful Violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681)

63. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. This claim is brought by Plaintiff on behalf of himself and all members of the National Class.

64. By the acts and omissions set forth herein, Defendant has willfully violated the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. ("FCRA").

65. Plaintiff and members of the National Class are consumers within the meaning of the FCRA, 15 U.S.C. § 1681a(c).

66. Defendant Equifax is a consumer reporting agency within the meaning of the FCRA, 15 U.S.C. § 1681a(f), because, among other things, it regularly engages in the practice, for monetary fees, of assembling and/or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

67. Plaintiff's and Class members' Personal Information is protected by the FCRA. The Personal Information is a consumer report within the meaning of the FCRA, 15 U.S.C. § 1681a(f).

68. The FCRA required Equifax to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under the FCRA, 15 U.S.C. § 1681b. None of the listed purposes includes furnishing consumer reports to unknown and unauthorized persons or entities such as the hackers who acquired the Personal Information in the data breach.

69. Equifax willfully failed to maintain reasonable procedures designed to limit furnishing of the Personal Information of Plaintiff and Class members to the purposes authorized under the FCRA.

70. Equifax violated the FCRA by furnishing consumer reports to hackers in the data breach and/or by willfully or recklessly allowing unauthorized entities to access Plaintiff's and National Class members' Protected Information.

71. Plaintiff and National Class members have been damaged by Equifax's willful and/or reckless violations of the FCRA.

72. Pursuant to 15 U.S.C. § 1681n(a)(1)(A), Plaintiff and National Class members are each entitled to their actual damages or statutory damages of not less than \$100 or greater than \$1,000.

73. Pursuant to 15 U.S.C. § 1681n(a)(2), Plaintiff and National Class members are entitled to punitive damages and to their attorney fees and costs of suit.

74. Pursuant to 15 U.S.C. § 1681n(a)(3), Plaintiff and National Class members are entitled to their attorney fees and costs of suit.

SECOND CAUSE OF ACTION

(Negligent Violation of the Fair Credit Reporting Act)

75. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. This claim is brought by Plaintiff on behalf of himself and all National Class members

76. By the acts and omissions set forth herein, Defendant has negligently violated the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("FCRA").

77. As set forth above, Plaintiff and National Class members are consumers and Defendant Equifax is a consumer reporting agency within the meaning of the FCRA.

78. Under the FCRA, 15 U.S.C. § 1681b, Equifax was required to maintain reasonable procedures designed to limit the furnishing of consumer reports, including the Personal Information, to the purposes listed therein, none of which allow furnishing consumer reports to unknown and unauthorized persons or entities.

79. Equifax failed to maintain reasonable procedures designed to limit furnishing of the Personal Information of Plaintiff and National Class members to the purposes authorized under the FCRA.

80. As a direct and proximate result of Defendant's negligence, unauthorized persons gained access to and acquired Plaintiff's and National Class members' Protected Information.

81. Plaintiff and Class members have been damaged by Equifax's negligent violations of the FCRA.

82. Accordingly, Plaintiff and National Class members are entitled to their actual damages, and are entitled to their attorney fees and costs of suit.

THIRD CAUSE OF ACTION

(Violation of the Security Breach Notification Law, Cal. Civil Code § 1798.82)

83. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. This claim is brought by Plaintiff on behalf of himself and all California Class members.

84. Defendant's acts and omissions violate the Security Breach Notification Law, Cal. Civil Code § 1798.82 *et seq.*

85. Defendant conducts business in California and owns or licenses digital data including, within the meaning of Cal. Civ. Code § 1798.82(h), the Personal Information of California residents, including Plaintiff.

86. Defendant's information security systems were breached, resulting in the theft of California Class members' Personal Information. Defendant learned of the breach no later than July 2017, and possibly months earlier, but has failed to send Plaintiff and individual California Class members timely written notice as required by Cal. Civ. Code § 1798.82, and has failed to provide the information required by law.

87. By failing to timely disclose to Plaintiff and each member of the proposed California Class in the most expedient manner possible that their Personal Information has been acquired by an unauthorized person, Defendant violated Cal. Civ. Code § 1798.82.

88. There was no lawful reason for the delay in notifying Plaintiff and California Class members of the data breach and providing the information required by Cal. Civ. Code § 1798.82.

89. As a direct and proximate result of Defendant's violations of Cal. Civ. Code § 1798.82, Plaintiff and California Class members have suffered harm and damages.

90. Plaintiff and California Class members are therefore entitled to damages, injunctive relief, and attorneys' fees and costs as prayed for hereunder.

//

//

//

//

FOURTH CAUSE OF ACTION

(Violation of the Customer Records Act, Cal. Civ. Code § 1798.80)

91. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. This claim is brought by Plaintiff on behalf of himself and all California Class members.

92. Defendant's acts and omissions violate the California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*

93. Equifax is a business that owns or licenses personal information about California residents within the meaning of Cal. Civ. Code § 1798.81.5.

94. By failing to implement and maintain appropriate and reasonable security procedures and practices to protect the Personal Information of Plaintiff and the California Class from unauthorized access and disclosure, Equifax violated Cal. Civ. Code § 1798.81.5.

95. As a result of Equifax's violation of Cal. Civ. Code § 1798.81.5, Plaintiff and California Class members have been injured.

96. Plaintiff and California Class members are therefore entitled to damages, injunctive relief, and reasonable attorneys' fees and costs pursuant to § 1798.84, as prayed for hereunder.

FIFTH CAUSE OF ACTION

(For Negligence and Negligent Failure to Warn)

97. Plaintiff realleges, as if fully set forth, each and every allegation set forth above, and pleads this cause of action on behalf of himself and all members of both Classes.

98. The actions of Defendant constitute negligence and/or negligent failure to warn.

99. Defendant owed a duty of care to Plaintiff and members of the Classes. Defendant breached that duty.

100. Among other things, Defendant failed to warn Plaintiff and members of the Classes that their Personal Information entrusted to Defendant was not properly protected and that Defendant did not maintain the security procedures and measures reasonable necessary to protect such data from exposure and theft.

101. Among other things, Defendant failed to implement and maintain the security procedures and measures reasonable necessary to protect Plaintiff's and Class members' Personal Information from exposure and theft.

102. Among other things, Defendant failed to notify Plaintiff and members of the Classes in a timely manner of the data breach and of the danger to them caused by the data breach.

103. Among other things, Defendant failed to implement and maintain the security procedures and protocols reasonable necessary to protect Plaintiff's and Class members' Personal Information from exposure and theft.

104. As a direct and proximate result of the practices, acts and omissions alleged herein, Plaintiff and members of the Classes have suffered injury and damages.

105. At all relevant times, Plaintiff and members of the Classes acted lawfully and with due care and did not contribute to the injuries suffered.

106. Because of the harm directly and proximately caused by the breaches of duty and/or acts and omissions described herein, Plaintiff and members of the Classes are entitled to damages and other appropriate relief, as prayed for hereunder.

SIXTH CAUSE OF ACTION

(Violations of the Unfair Competition Law, Bus. & Prof. Code §§ 17200, *et seq.*)

107. Plaintiff realleges, as if fully set forth, each and every allegation set forth above, and pleads this cause of action on behalf of himself and all members of the California Class.

108. Defendant's business practices as complained of herein violate the Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200, *et seq.* ("UCL").

109. Defendant's practices constitute "unlawful" business practices in violation of the UCL because, among other things, they violate statutory law and the common law.

110. Defendant's actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, they are immoral, unethical, oppressive, unconscionable, unscrupulous or substantially injurious to consumers, and/or any utility of such practices is outweighed by the harm caused consumers.

111. Defendant's actions and practices constitute "fraudulent" business practices in violation of the UCL because, among other things, they have a capacity and tendency to deceive members of the public.

112. As a result of Defendant's wrongful business practices, Plaintiff and California Class members have suffered injury in fact.

113. Defendant's wrongful business practices present an ongoing and continuing threat to the general public.

114. Accordingly, Plaintiff is entitled to and prays for judgment and for equitable relief for himself and California Class members, and, where appropriate, members of the general public; and for attorneys' fees and costs of suit, as set forth hereunder.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Classes pray for relief and judgment against Defendant, as follows:

- A. Certifying the Classes pursuant to Rule 23 of the Federal Rules of Civil Procedure, certifying Plaintiff as representative of the Classes and designating his counsel as counsel for the Classes;
- B. Awarding Plaintiff and the Classes compensatory damages, in an amount exceeding \$5,000,000, to be determined by proof;
- C. Awarding Plaintiff and the Classes statutory damages;
- D. Awarding Plaintiff and the Classes punitive damages;
- E. For declaratory and equitable relief, including restitution and disgorgement;
- F. For an order enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;
- G. For injunctive relief requiring Defendant to take steps to repair the injury caused by its wrongful conduct;
- H. Awarding Plaintiff and the Classes the costs of prosecuting this action, including expert witness fees;
- I. Awarding Plaintiff and the Classes reasonable attorney fees;
- J. Awarding pre-judgment and post-judgment interest; and

1 K. Granting other relief as this Court may deem just and proper.

2
3 **DEMAND FOR JURY TRIAL**

4 Plaintiff Malcolm B. Feied hereby demands trial by jury of all claims so triable.

5
6 Respectfully submitted,

7 Date: September 22, 2017

By: /s/ Gordon M. Fauth, Jr.

Gordon M. Fauth, Jr.

Of Counsel

Rosanne L. Mah

Of Counsel

10 **FINKELSTEIN THOMPSON LLP**

100 Pine Street, Suite 1250

San Francisco, California 94111

Direct Telephone: (510) 238-9610

Telephone: (415) 398-8700

Facsimile: (415) 398-8704

14 Attorneys for Individual and Representative
15 Plaintiff Malcolm B. Feied